

Secrecy Rate Region of the Broadcast Channel with an Eavesdropper

Ghadamali Bagherikaram, Abolfazl S. Motahari, Amir K. Khandani
 Coding and Signal Transmission Laboratory,
 Department of Electrical and Computer Engineering,
 University of Waterloo, Waterloo, Ontario, N2L 3G1
 Emails: {gbagheri,abolfazl,khandani}@cst.uwaterloo.ca

Abstract

In this paper, we consider a scenario where a source node wishes to broadcast two confidential messages to two receivers, while a wire-tapper also receives the transmitted signal. This model is motivated by wireless communications, where individual secure messages are broadcast over open media and can be received by any illegitimate receiver. The secrecy level is measured by the equivocation rate at the eavesdropper. We first study the general (non-degraded) broadcast channel with an eavesdropper. We present an inner bound on the secrecy capacity region for this model. This inner bound is based on a combination of random binning, and the Gelfand-Pinsker binning. We further study the situation in which the channels are degraded. For the degraded broadcast channel with an eavesdropper, we present the secrecy capacity region. Our achievable coding scheme is based on Cover's superposition scheme and random binning. We refer to this scheme as the Secret Superposition Scheme. Our converse proof is based on a combination of the converse proof of the conventional degraded broadcast channel and Csiszar Lemma. We then assume that the channels are Additive White Gaussian Noise (AWGN) and show that the Secret Superposition Scheme with Gaussian codebook is optimal. The converse proof is based on Costa's entropy power inequality. Finally, we use a broadcast strategy for the slowly fading wire-tap channel when only the eavesdropper's channel is fixed and known at the transmitter. We derive the optimum power allocation for the coding layers, which maximizes the total average rate.

I. INTRODUCTION

The notion of information theoretic secrecy in communication systems was first introduced by Shannon in [1]. The information theoretic secrecy requires that the received signal of the eavesdropper does not provide any information about the transmitted messages. Shannon considered a pessimistic situation where both the intended receiver and the eavesdropper have direct access to the transmitted signal (which is called ciphertext). Under these circumstances, he proved a negative result showing that perfect secrecy can be achieved only when the entropy of the secret key is greater than, or equal to, the entropy of the message. In modern cryptography, all practical cryptosystems are based on Shannon's pessimistic assumption. Due to practical constraints, secret keys are much shorter than messages; therefore, these practical cryptosystems are theoretically susceptible to breaking by attackers. The goal of designing such practical ciphers, however, is to guarantee that no efficient algorithm exists for breaking them.

Wyner in [2] showed that the above negative result is a consequence of Shannon's restrictive assumption that the adversary has access to precisely the same information as the legitimate receiver. Wyner considered a scenario in which a wire-tapper receives the transmitted signal over a degraded channel with respect to the legitimate receiver's channel. He further assumed that the wire-tapper has no computational limitations and knows the codebook used by the transmitter. He measured the level of ignorance at the eavesdropper by its equivocation and characterized the capacity-equivocation region. Interestingly, a non-negative perfect secrecy capacity is always achievable for this scenario.

The secrecy capacity for the Gaussian wire-tap channel is characterized by Leung-Yan-Cheong in [3]. Wyner's work is then extended to the general (non-degraded) broadcast channel with confidential messages by Csiszar and Korner [4]. They considered transmitting confidential information to the legitimate receiver while transmitting common information to both the legitimate receiver and the wire-tapper. They established a capacity-equivocation region for this channel. The BCC has recently been further studied in [5]–[7], where the source node transmits a common message to both receivers, along with two additional confidential messages, each aimed at one of the two receivers. Here, the confidentiality of each message is measured with respect to the other user, and there is no external eavesdropper.

The fading wire-tap channel is investigated in [8] where the source-to-destination channel and the source-to-eavesdropper channel are corrupted by multiplicative fading gain coefficients, in addition to additive white Gaussian noise. In this work, channels are fast fading and the Channel State Information (CSI) of the legitimate receiver is available at the transmitter. The perfect secrecy capacity is derived for two different scenarios regarding the availability of the eavesdropper's CSI. Moreover,

¹Financial support provided by Nortel and the corresponding matching funds by the Natural Sciences and Engineering Research Council of Canada (NSERC), and Ontario Centres of Excellence (OCE) are gratefully acknowledged.

the optimal power control policy is obtained for the different scenarios. The effect of the slowly fading channel on the secrecy capacity of a conventional wire-tap channel is studied in [9], [10]. In these works, it is assumed that the fading is quasi-static and the transmitter does not know the fading gains. The outage probability, which is the probability that the main channel is stronger than the eavesdropper's channel, is defined in these works. In an outage strategy, the transmission rate is fixed and the information is detected when the instantaneous main channel is stronger than the instantaneous eavesdropper's channel; otherwise, either nothing is decoded at the legitimate receiver, or the information is leaked to the eavesdropper. The term outage capacity refers to the maximum achievable average rate. In [11], a broadcast strategy for the slowly fading Gaussian point to point channel is introduced. In this strategy, the transmitter uses a layered coding scheme and the receiver is viewed as a continuum of ordered users.

In [15], the wire-tap channel is extended to the parallel broadcast channels and also to the fading channels with multiple receivers. In [15], the secrecy constraint is a perfect equivocation for each of the messages, even if all the other messages are revealed to the eavesdropper. The secrecy sum capacity for a reverse broadcast channel is derived subject to this restrictive assumption. The notion of the wire-tap channel is also extended to multiple access channels [16]–[19], relay channels [20]–[23], parallel channels [24] and Multiple-Input Multiple-Output channels [25]–[31]. Some other related works on the communication of confidential messages can be found in [32]–[36].

In this paper, we consider a scenario where a source node wishes to broadcast two confidential messages to two receivers, while a wire-tapper also receives the transmitted signal. This model is motivated by wireless communications, where individual secure messages are broadcast over shared media and can be received by any illegitimate receiver. In fact, we simplify the restrictive constraint imposed in [15] and assume that the eavesdropper does not have access to the other messages. We first study the general broadcast channel with an eavesdropper. We present an achievable rate region for this channel. Our achievable coding scheme is based on a combination of random binning and the Gelfand-Pinsker binning [37]. This scheme matches the Marton's inner bound [38] on the broadcast channel without confidentiality constraint. We further study the situation where the channels are physically degraded and characterize the corresponding secrecy capacity region. Our achievable coding scheme is based on Cover's superposition coding [39] and random binning. We refer to this scheme as the Secret Superposition Coding. This capacity region matches the capacity region of the degraded broadcast channel without any security constraint. It also matches the secrecy capacity of the wire-tap channel. We also characterize the secrecy capacity region when the channels are additive white Gaussian noise. We show that the secret superposition of Gaussian codebooks is the optimal choice. Based on the rate characterization of the secure broadcast channel, we then use broadcast strategy for the slow fading wire-tap channel when only the eavesdropper's channel is fixed and known at the transmitter. In broadcast strategy, a source node sends secure layers of coding and the receiver is viewed as a continuum of ordered users. We derive optimum power allocation for the layers which maximizes the total average rate.

In [40], we published a conference version of this work where the achievable rate region of the general broadcast channel with an eavesdropper and the secrecy capacity region of the degraded one were addressed. However, we later became aware that reference [41], [42] had considered a similar model as used in this paper and had independently characterized the secrecy capacity region of the broadcast channel (when the channels are degraded). They also generalized their results to the parallel degraded broadcast channel with an eavesdropper. Independently and parallel to our work, reference [43] considered the Gaussian broadcast channel with an eavesdropper and characterized its capacity region. Authors of [43] provided two methods for their converse proof. The first one uses the alternative representation of the mutual information as an integration of the minimum-mean-square-error (MMSE), as well as the properties of the MMSE. The second one uses the relationship between the differential entropy and the Fisher information via the de Bruin identity, along with the properties of the Fisher information. In this work, however, we use Costa's entropy power inequality to provide the converse proof.

The rest of the paper is organized as follows: in section II we introduce the system model. In section III we provide an inner bound on the secrecy capacity region when the channels are not degraded. In section IV we specialize our channel to the degraded ones and establish the secrecy capacity region. In section V we derive the secrecy capacity region when the channels are AWGN. Based on the secrecy capacity region of the AWGN channel, in section VI we use a broadcast strategy for the slow fading wire-tap channel when the transmitter only knows the eavesdropper's channel. Finally, section VII concludes the paper.

II. PRELIMINARIES

In this paper, random variables are denoted by capital letters (e.g. X) and their realizations are denoted by corresponding lower case letters (e.g. x). The finite alphabet of a random variable is denoted by a script letter (e.g. \mathcal{X}) and its probability distribution is denoted by $P(x)$. The vectors will be written as $x^n = (x_1, x_2, \dots, x_n)$, where subscripted letters denote the components and superscripted letters denote the vector. Bold capital letters represent matrices (e.g. \mathbf{A}). The notation x^{i-1} denotes the vector $(x_1, x_2, \dots, x_{i-1})$ and the notation \tilde{x}^i denotes the vector $(x_i, x_{i+1}, \dots, x_n)$. A similar notation will be used for random variables and random vectors.

Consider a Broadcast Channel with an eavesdropper (BCE) as depicted in Fig. 1. In this confidential setting, the transmitter wishes to send two independent messages (W_1, W_2) to the respective receivers in n uses of the channel and prevent the

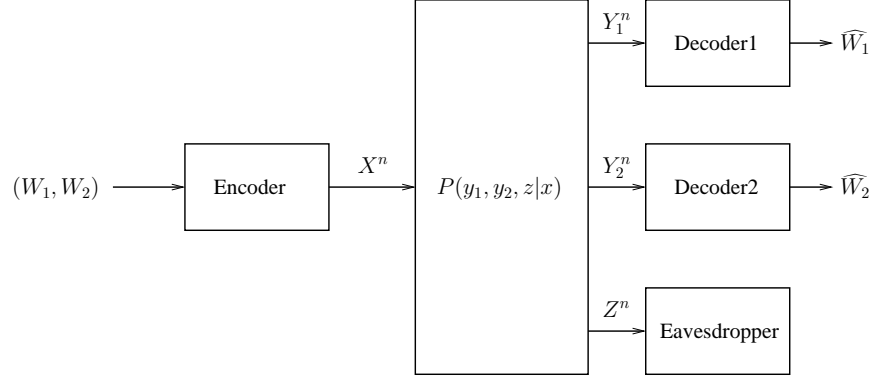


Fig. 1. Broadcast Channel with an Eavesdropper

eavesdropper from having any information about the messages. A discrete memoryless broadcast channel with an eavesdropper is represented by $(\mathcal{X}, P, \mathcal{Y}_1, \mathcal{Y}_2, \mathcal{Z})$ where, \mathcal{X} is the finite input alphabet set, \mathcal{Y}_1 , \mathcal{Y}_2 and \mathcal{Z} are three finite output alphabet sets, and P is the channel transition probability $P(y_1, y_2, z|x)$. The input of the channel is $x^n \in \mathcal{X}^n$ and the outputs are $y_1^n \in \mathcal{Y}_1^n$, $y_2^n \in \mathcal{Y}_2^n$, and $z^n \in \mathcal{Z}^n$ for Receiver 1, Receiver 2, and the eavesdropper, respectively. The channel is discrete memoryless in the sense that

$$P(y_1^n, y_2^n, z^n|x^n) = \prod_{i=1}^n P(y_{1,i}, y_{2,i}, z_i|x_i). \quad (1)$$

A $((2^{nR_1}, 2^{nR_2}), n)$ code for a broadcast channel with an eavesdropper consists of a stochastic encoder

$$f : (\{1, 2, \dots, 2^{nR_1}\} \times \{1, 2, \dots, 2^{nR_2}\}) \rightarrow \mathcal{X}^n, \quad (2)$$

and two decoders,

$$g_1 : \mathcal{Y}_1^n \rightarrow \{1, 2, \dots, 2^{nR_1}\} \quad (3)$$

and

$$g_2 : \mathcal{Y}_2^n \rightarrow \{1, 2, \dots, 2^{nR_2}\}. \quad (4)$$

The average probability of error is defined as the probability that the decoded messages are not equal to the transmitted messages; that is,

$$P_e^{(n)} = P(g_1(Y_1^n) \neq W_1 \cup g_2(Y_2^n) \neq W_2). \quad (5)$$

The knowledge that the eavesdropper can extract about W_1 and W_2 from its received signal Z^n is measured by

$$I(Z^n, W_1) = H(W_1) - H(W_1|Z^n), \quad (6)$$

$$I(Z^n, W_2) = H(W_2) - H(W_2|Z^n), \quad (7)$$

and

$$I(Z^n, (W_1, W_2)) = H(W_1, W_2) - H(W_1, W_2|Z^n). \quad (8)$$

Perfect secrecy revolves around the idea that the eavesdropper should not obtain any information about the transmitted messages. Perfect secrecy thus requires that

$$I(Z^n, W_1) = 0 \Leftrightarrow H(W_1) = H(W_1|Z^n),$$

$$I(Z^n, W_2) = 0 \Leftrightarrow H(W_2) = H(W_2|Z^n),$$

and

$$I(Z^n, (W_1, W_2)) = 0 \Leftrightarrow H(W_1, W_2) = H(W_1, W_2|Z^n).$$

where $n \rightarrow \infty$. The secrecy levels of confidential messages W_1 and W_2 are measured at the eavesdropper in terms of equivocation rates which are defined as follows:

Definition 1 The equivocation rates R_{e1} , R_{e2} and R_{e12} for the broadcast channel with an eavesdropper are:

$$R_{e1} = \frac{1}{n} H(W_1|Z^n),$$

$$R_{e2} = \frac{1}{n} H(W_2|Z^n),$$

$$R_{e12} = \frac{1}{n} H(W_1, W_2|Z^n).$$

The perfect secrecy rates R_1 and R_2 are the amount of information that can be sent to the legitimate receivers in a reliable and confidential manner.

Definition 2 A secrecy rate pair (R_1, R_2) is said to be achievable if for any $\epsilon > 0, \epsilon_1 > 0, \epsilon_2 > 0, \epsilon_3 > 0$, there exists a sequence of $((2^{nR_1}, 2^{nR_2}), n)$ codes, such that for sufficiently large n , we have:

$$P_e^{(n)} \leq \epsilon, \quad (9)$$

$$R_{e1} \geq R_1 - \epsilon_1, \quad (10)$$

$$R_{e2} \geq R_2 - \epsilon_2, \quad (11)$$

$$R_{e12} \geq R_1 + R_2 - \epsilon_3. \quad (12)$$

In the above definition, the first condition concerns the reliability, while the other conditions guarantee perfect secrecy for each individual message and the combination of the two messages, respectively. Since the messages are independent of each other, the conditions of (10) and (12) or (11) and (12) are sufficient to provide perfect secrecy. The capacity region is defined as follows.

Definition 3 The capacity region of the broadcast channel with an eavesdropper is the closure of the set of all achievable rate pairs (R_1, R_2) .

III. ACHIEVABLE RATES FOR GENERAL BCE

In this section, we consider the general broadcast channel with an eavesdropper and present an achievable rate region. Our achievable coding scheme is based on a combination of the random binning, superposition coding, rate splitting, and Gelfand-Pinsker binning schemes [37]. Our binning approach is supplemented with superposition coding to accommodate the common message. We call this scheme the Secret Superposition Scheme. An additional binning is introduced for the confidentiality of private messages. We note that these double binning techniques have been used by various authors for secret communication (see e.g. [5], [7]). The following theorem illustrates the achievable rate region for this channel.

Theorem 1 Let \mathbb{R}_I denote the union of all non-negative rate pairs (R_0, R_1, R_2) satisfying

$$\begin{aligned} R_0 &\leq \min\{I(U; Y_1), I(U; Y_2)\} - I(U; Z), \\ R_1 + R_0 &\leq I(V_1; Y_1|U) - I(V_1; Z|U) + \min\{I(U; Y_1), I(U; Y_2)\} - I(U; Z), \\ R_2 + R_0 &\leq I(V_2; Y_2|U) - I(V_2; Z|U) + \min\{I(U; Y_1), I(U; Y_2)\} - I(U; Z), \\ R_1 + R_2 + R_0 &\leq I(V_1; Y_1|U) + I(V_2; Y_2|U) - I(V_1, V_2; Z|U) - I(V_1; V_2|U) + \min\{I(U; Y_1), I(U; Y_2)\} - I(U; Z), \end{aligned}$$

over all joint distributions $P(u)P(v_1, v_2|u)P(x|v_1, v_2)P(y_1, y_2, z|x)$. Any rate pair $(R_0, R_1, R_2) \in \mathbb{R}_I$ is then achievable for the broadcast channel with an eavesdropper and with common information.

Please see Appendix I for the proof.

Remark 1 If we remove the secrecy constraints by removing the eavesdropper, the above rate region becomes Marton's achievable region with common information for the general broadcast channel.

Remark 2 If we remove one of the users, e.g. user 2 and the common message, then we get Csiszar and Korner's secrecy capacity for the other user.

IV. THE CAPACITY REGION OF THE DEGRADED BCE

In this section, we consider the degraded broadcast channel with an eavesdropper and establish its secrecy capacity region.

Definition 4 A broadcast channel with an eavesdropper is said to be physically degraded, if $X \rightarrow Y_1 \rightarrow Y_2 \rightarrow Z$ forms a Markov chain. In other words, we have

$$P(y_1, y_2, z|x) = P(y_1|x)P(y_2|y_1)P(z|y_2).$$

Definition 5 A broadcast channel with an eavesdropper is said to be stochastically degraded if its conditional marginal distributions are the same as that of a physically degraded broadcast channel, i.e., if there exist two distributions $P'(y_2|y_1)$ and $P'(z|y_2)$, such that

$$P(y_2|x) = \sum_{y_1} P(y_1|x) P'(y_2|y_1),$$

$$P(z|x) = \sum_{y_2} P(y_2|x) P'(z|y_2).$$

Lemma 1 *The secrecy capacity region of a broadcast channel with an eavesdropper depends only on the conditional marginal distributions $P(y_1|x)$, $P(y_2|x)$ and $P(z|x)$.*

Proof: It suffices to show that the error probability of $P_e^{(n)}$ and the equivocations of $H(W_1|Z^n)$, $H(W_2|Z^n)$ and $H(W_1, W_2|Z^n)$ are only functions of the marginal distributions when we use the same codebook and encoding schemes. Note that

$$\max\{P_{e,1}^{(n)}, P_{e,2}^{(n)}\} \leq P_e^{(n)} \leq P_{e,1}^{(n)} + P_{e,2}^{(n)}.$$

Hence, $P_e^{(n)}$ is small if, and only if, both $P_{e,1}^{(n)}$ and $P_{e,2}^{(n)}$ are small. On the other hand, for a given codebook and encoding scheme, the decoding error probabilities $P_{e,1}^{(n)}$ and $P_{e,2}^{(n)}$ and the equivocation rates depend only on marginal channel probability densities $P_{Y_1|X}$, $P_{Y_2|X}$ and $P_{Z|X}$. Thus, the same code and encoding scheme gives the same $P_e^{(n)}$ and equivocation rates. ■

In the following theorem, we fully characterize the capacity region of the physically degraded broadcast channel with an eavesdropper.

Theorem 2 *The capacity region for transmitting independent secret information over the degraded broadcast channel is the convex hull of the closure of all (R_1, R_2) satisfying*

$$R_1 \leq I(X; Y_1|U) - I(X; Z|U), \quad (13)$$

$$R_2 \leq I(U; Y_2) - I(U; Z), \quad (14)$$

for some joint distribution $P(u)P(x|u)P(y_1, y_2, z|x)$.

Please refer to Appendix II for the proof.

Remark 3 *If we remove the secrecy constraints by removing the eavesdropper, then the above theorem becomes the capacity region of the degraded broadcast channel.*

The coding scheme is based on Cover's superposition coding and random binning. We refer to this scheme as the Secure Superposition Coding scheme. The available resources at the encoder are used for two purposes: to confuse the eavesdropper so that perfect secrecy can be achieved for both layers, and to transmit the messages into the main channels. To satisfy confidentiality, the randomization used in the first layer is fully exploited in the second layer. This makes an increase of $I(U; Z)$ in the bound of R_1 .

Remark 4 *As Lemma 2 bounds the secrecy rates for the general broadcast channel with an eavesdropper then, Theorem 2 is true when only the legitimate receivers are degraded.*

V. CAPACITY REGION OF GAUSSIAN BCE

In this section, we consider the Gaussian Broadcast Channel with an Eavesdropper (G-BCE). Note that optimizing (13) and (14) for AWGN channels involves solving a nonconvex functional. Usually nontrivial techniques and strong inequalities are used to solve the optimization problems of this type. In [3], Leung-Yan-Cheong successfully evaluated the capacity expression of the wire-tap channel by using the entropy power inequality [44], [45]. Alternatively, it can also be evaluated using a classical result from the Estimation Theory and the relationship between mutual information and minimum mean-squared error estimation. On the other hand, the entropy power inequality is sufficient to establish the converse proof of a Gaussian broadcast channel without secrecy constraint. Unfortunately, the traditional entropy power inequality does not extend to the secure multi-user case. Here, by using Costa's version of the entropy power inequality, we show that secret superposition coding with Gaussian codebook is optimal.

Figure 2 shows the channel model. At time i the received signals are $Y_{1i} = X_i + N_{1i}$, $Y_{2i} = X_i + N_{2i}$ and $Z_i = X_i + N_{3i}$, where N_{ji} is a Gaussian random variable with zero mean and $\text{Var}(N_{ji}) = \sigma_j^2$ for $j = 1, 2, 3$. Here $\sigma_1^2 \leq \sigma_2^2 \leq \sigma_3^2$. Assume that the transmitted power is limited to $E[X^2] \leq P$. Since the channels are degraded, the received signals can alternatively be written as $Y_{1i} = X_i + N_{1i}$, $Y_{2i} = Y_{1i} + N'_{2i}$ and $Z_i = Y_{2i} + N'_{3i}$, where N_{1i} 's are i.i.d $\mathcal{N}(0, \sigma_1^2)$, N'_{2i} 's are i.i.d $\mathcal{N}(0, \sigma_2^2 - \sigma_1^2)$, and N'_{3i} 's are i.i.d $\mathcal{N}(0, \sigma_3^2 - \sigma_2^2)$. Fig. 3 shows the equivalent channels for the G-BCE. The following theorem illustrates the secrecy capacity region of G-BCE.

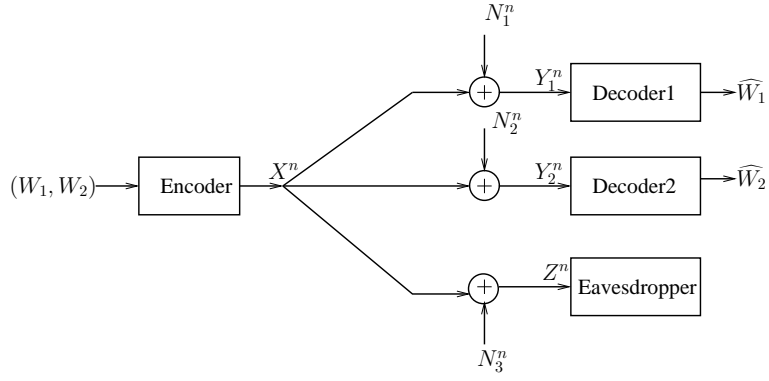


Fig. 2. Gaussian Broadcast Channel with an Eavesdropper(G-BCE)

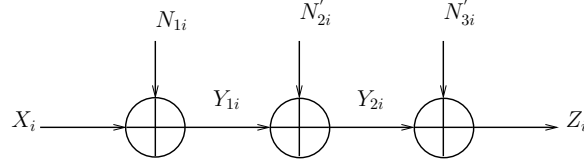


Fig. 3. Equivalent Channels for the G-BCE

Theorem 3 *The secrecy capacity region of the G-BCE is given by the set of rates pairs (R_1, R_2) satisfying*

$$R_1 \leq C\left(\frac{\alpha P}{\sigma_1^2}\right) - C\left(\frac{\alpha P}{\sigma_3^2}\right), \quad (15)$$

$$R_2 \leq C\left(\frac{(1-\alpha)P}{\alpha P + \sigma_2^2}\right) - C\left(\frac{(1-\alpha)P}{\alpha P + \sigma_3^2}\right). \quad (16)$$

for some $\alpha \in [0, 1]$.

Please see Appendix III for the proof.

Figure 4 shows the capacity region of a degraded Gaussian broadcast channel with and without secrecy constraint. In this figure $P = 20$, $N_1 = 0.9$, $N_2 = 1.5$ and $N_3 = 4$.

VI. A MULTILEVEL CODING APPROACH TO THE SLOWLY FADING WIRE-TAP CHANNEL

In this section, we use the secure degraded broadcast channel from the previous section to develop a new broadcast strategy for a slow fading wire-tap channel. This strategy aims to maximize the average achievable rate where the main channel

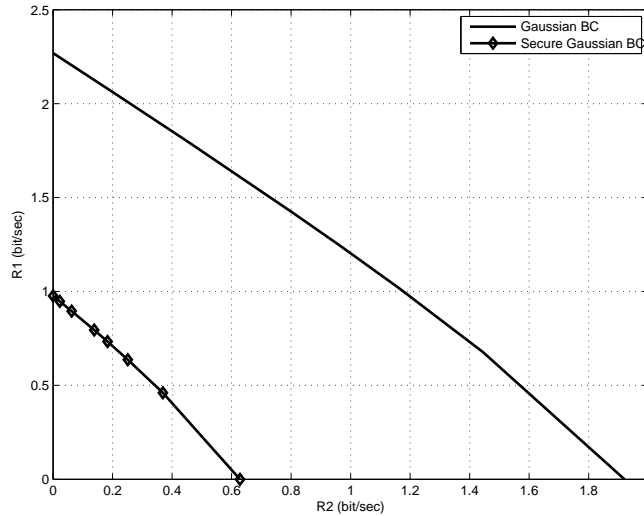


Fig. 4. Secret/Non-Secret Capacity Region of a Degraded Broadcast Channel

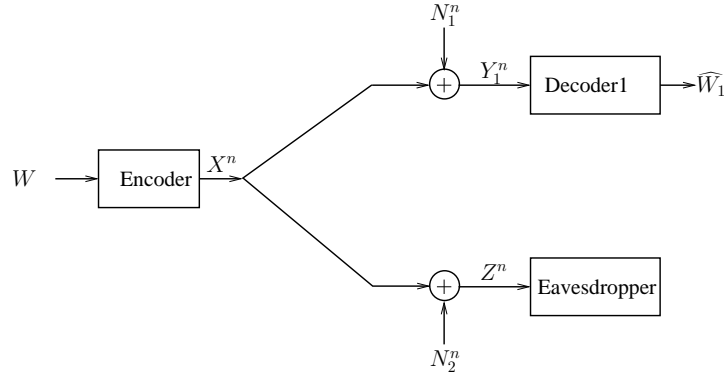


Fig. 5. Gaussian Wire-tap Channel

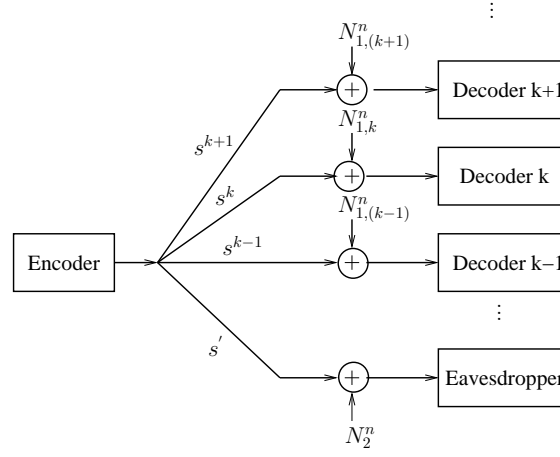


Fig. 6. Equivalent Broadcast Channel Model.

state information is not available at the transmitter. By assuming that there is an infinite number of ordered receivers which correspond to different channel realizations, we propose a secret multilevel coding scheme that maximizes the underlying objective function. First, some preliminaries and definitions are given, and then the proposed multilevel coding scheme is described. Here, we follow the steps of the broadcast strategy for the slowly fading point-to-point channel of [11]. This method is used in several other papers; see, e.g., [12]–[14].

A. Channel Model

Consider a wire-tap channel as depicted in Fig. 5. The transmitter wishes to communicate with the destination in the presence of an eavesdropper. At time i , the signal received by the destination and the eavesdropper are given as follows

$$\begin{aligned} Y_i &= h_M X_i + N_{1i} \\ Z_i &= h_E X_i + N_{2i} \end{aligned} \quad (17)$$

where X_i is the transmitted symbol and h_M, h_E are the fading coefficients from the source to the legitimate receiver and to the eavesdropper, respectively. The fading power gains of the main and eavesdropper channels are given by $s = |h_M|^2$ and $s' = |h_E|^2$, respectively. N_{1i}, N_{2i} are the additive noise samples, which are Gaussian i.i.d with zero mean and unit variance. We assume that the channels are slowly fading, and also assume that the transmitter knows only channel state information of the eavesdropper channel. A motivation for this assumption is that when both channels are unknown at the transmitter, we assume that $s' = |h_E|^2$ denotes the best-case eavesdropper channel gain. For each realization of h_M there is an achievable rate. Since the transmitter has no information about the main channel and the channels are slowly fading, then the system is non-ergodic. Here, we are interested in the average rate for various independent transmission blocks. The average shall be calculated over the distribution of h_M .

B. The Secret Multilevel Coding Approach

An equivalent broadcast channel for our channel is depicted in Fig. 6. wherein the transmitter sends an infinite number of

secure layers of coded information. The receiver is equivalent to a continuum of ordered users. For each channel realization h_M^k with the fading power gain s^k , the information rate is $R(s^k, s')$. We drop the superscript k , and the realization of the fading power random variable S is denoted by s . Therefore, the transmitter views the main channel as a secure degraded Gaussian broadcast channel with an infinite number of receivers. The result of the previous section for the two receivers can easily be extended to an arbitrary number of users. According to theorem 3, the incremental differential secure rate is then given by

$$dR(s, s') = \left[\frac{1}{2} \log \left(1 + \frac{s\rho(s)ds}{1+sI(s)} \right) - \frac{1}{2} \log \left(1 + \frac{s'\rho(s)ds}{1+s'I(s)} \right) \right]^+, \quad (18)$$

where $\rho(s)ds$ is the transmit power of a layer parameterized by s , intended for receiver s . As $\log(1+x) \approx x$ for $x \leq 1$ then the log function may be discarded. The function $I(s)$ represents the interference noise of the receivers indexed by $u > s$ which cannot be canceled at receiver s . The interference at receiver s is therefore given by

$$I(s) = \int_s^\infty \rho(u)du. \quad (19)$$

The total transmitted power is the summation of the power assigned to the layers

$$P = I(0) = \int_0^\infty \rho(u)du. \quad (20)$$

The total achievable rate for a fading realization s is an integration of the incremental rates over all receivers, which can successfully decode the respective layer

$$R(s, s') = \frac{1}{2} \int_0^s \left[\frac{u\rho(u)du}{1+uI(u)} - \frac{s'\rho(u)du}{1+s'I(u)} \right]^+. \quad (21)$$

Our goal is to maximize the total average rate over all fading realizations with respect to the power distribution $\rho(s)$ (or equivalently, with respect to $I(u)$, $u \geq 0$) under the power constraint of 20. The optimization problem may be written as

$$\begin{aligned} R_{\max} &= \max_{I(u)} \int_0^\infty R(u, s')f(u)du, \\ s.t. \\ P &= I(0) = \int_0^\infty \rho(u)du, \end{aligned} \quad (22)$$

where $f(u)$ is the probability distribution function (pdf) of the power gain S . Noting that the cumulative distribution function (cdf) is $F(u) = \int_0^u f(a)da$, the optimization problem may be written as

$$\begin{aligned} R_{\max} &= \frac{1}{2} \max_{I(u)} \int_0^\infty (1 - F(u))G(u)du, \\ s.t. \\ P &= I(0) = \int_0^\infty \rho(u)du, \end{aligned} \quad (23)$$

where $G(u) = \left[\frac{u}{1+uI(u)} - \frac{s'}{1+s'I(u)} \right]^+ \rho(u)$. Note that $\rho(u) = -I'(u)$. Therefore, the functional in (23) may be written as

$$\begin{aligned} J(x, I(x), I'(x)) &= \\ &= -(1 - F(x)) \left[\frac{x}{1+xI(x)} - \frac{s'}{1+s'I(x)} \right]^+ I'(x). \end{aligned} \quad (24)$$

The necessary condition for the maximization of an integral of J over x is

$$J_I - \frac{d}{dx} J_{I'} = 0, \quad (25)$$

where J_I means the derivation of function J with respect to I , and similarly $J_{I'}$ is the derivation of J with respect to I' . After some manipulations, the optimum $I(x)$ is given by

$$I(x) = \begin{cases} \frac{1-F(x)-(x-s')f(x)}{s'(1-F(x))+x(x-s')f(x)}, & \max\{s', x_0\} \leq x \leq x_1; \\ 0, & \text{otherwise,} \end{cases}$$

where x_0 is determined by $I(x_0) = P$, and x_1 by $I(x_1) = 0$.

As a special case, consider the Rayleigh flat fading channel. The random variable S is exponentially distributed with

$$f(s) = e^{-s}, \quad F(s) = 1 - e^{-s}, \quad s \geq 0. \quad (26)$$

Substituting $f(s)$ and $F(s)$ into the optimum $I(s)$ and taking the derivative with respect to the fading power s yields the following optimum transmitter power policy

$$\rho(s) = -\frac{d}{ds}I(s) = \begin{cases} \frac{-s^2 + 2(s'+1)s - s'^2}{(s^2 - s's + s')^2}, & \max\{s', s_0\} \leq s \leq s_1; \\ 0, & \text{otherwise,} \end{cases}$$

where s_0 is the solution of the equation $I(s_0) = P$, which is

$$s_0 = \frac{-1 + Ps' + \sqrt{P^2 s'^2 + 2P(1-2P)s' + 4P + 1}}{2P},$$

and s_1 is determined by $I(s_1) = 0$, which is

$$s_1 = 1 + s'.$$

VII. CONCLUSION

A generalization of the wire-tap channel in the case of two receivers and one eavesdropper was considered. We established an inner bound for the general (non-degraded) case. This bound matches Marton's bound on broadcast channels without security constraint. Furthermore, we considered the scenario in which the channels are degraded. We established the perfect secrecy capacity region for this case. The achievability coding scheme is a secret superposition scheme where randomization in the first layer helps the secrecy of the second layer. The converse proof combines the converse proof for the degraded broadcast channel without security constraint, and the perfect secrecy constraint. We proved that the secret superposition scheme with the Gaussian codebook is optimal in AWGN-BCE. The converse proof is based on Costa's entropy power inequality and Csiszar lemma. Based on the rate characterization of the AWGN-BCE, the broadcast strategy for the slowly fading wire-tap channel were used. In this strategy, the transmitter only knows the eavesdropper's channel and the source node sends secure layered coding. The receiver is viewed as a continuum of ordered users. We derived the optimum power allocation for the layers, which maximizes the total average rate.

APPENDIX I

PROOF OF THEOREM 1

We split the private message $W_1 \in \{1, 2, \dots, 2^{nR_1}\}$ into $W_{11} \in \{1, 2, \dots, 2^{nR_{11}}\}$ and $W_{10} \in \{1, 2, \dots, 2^{nR_{10}}\}$, and $W_2 \in \{1, 2, \dots, 2^{nR_2}\}$ into $W_{22} \in \{1, 2, \dots, 2^{nR_{22}}\}$ and $W_{20} \in \{1, 2, \dots, 2^{nR_{20}}\}$, respectively. W_{11} and W_{22} are only to be decoded by the intended receivers, while W_{10} and W_{20} are to be decoded by both receivers. Now, we combine (W_{10}, W_{20}, W_0) into a single auxiliary variable U . The messages W_{11} and W_{22} are represented by auxiliary variables V_1 and V_2 , respectively. Here, $R_{10} + R_{11} = R_1$ and $R_{20} + R_{22} = R_2$.

1) *Codebook Generation*: The structure of the encoder is depicted in Fig.7. Fix $P(u)$, $P(v_1|u)$, $P(v_2|u)$ and $P(x|v_1, v_2)$. The stochastic encoding is as follows. Define

$$\begin{aligned} L_{11} &= I(V_1; Y_1|U) - I(V_1; Z, V_2|U), \\ L_{12} &= I(V_1; Z|V_2, U), \\ L_{21} &= I(V_2; Z|V_1, U) \\ L_{22} &= I(V_2; Y_2|U) - I(V_2; Z, V_1|U), \\ L_3 &= I(V_1; V_2|U) - \epsilon, \end{aligned}$$

Note that,

$$\begin{aligned} L_{11} + L_{12} + L_3 &= I(V_1; Y_1|U) - \epsilon, \\ L_{22} + L_{21} + L_3 &= I(V_2; Y_2|U) - \epsilon, \end{aligned}$$

We first prove the case where

$$R_{11} \geq L_{11} \geq 0, \quad (27)$$

$$R_{22} \geq L_{22} \geq 0. \quad (28)$$

Generate $2^{n(R_{10}+R_{20}+R_0)}$ independent and identically distributed (i.i.d) sequences $u^n(k)$ with $k \in \{1, 2, \dots, 2^{R_{10}+R_{20}+R_0}\}$, according to the distribution $P(u^n) = \prod_{i=1}^n P(u_i)$. For each codeword $u^n(k)$, generate $2^{L_{11}+L_{12}+L_3}$ i.i.d codewords $v_1^n(i, i', i'')$, with $i \in \{1, 2, \dots, 2^{nL_{11}}\}$, $i' \in \{1, 2, \dots, 2^{nL_{12}}\}$ and $i'' \in \{1, 2, \dots, 2^{nL_3}\}$, according to $P(v_1^n|u^n) = \prod_{i=1}^n P(v_{1i}|u_i)$. The indexing presents an alternative interpretation of binning. Randomly distribute these sequences of v_1^n into $2^{nL_{11}}$ bins indexed

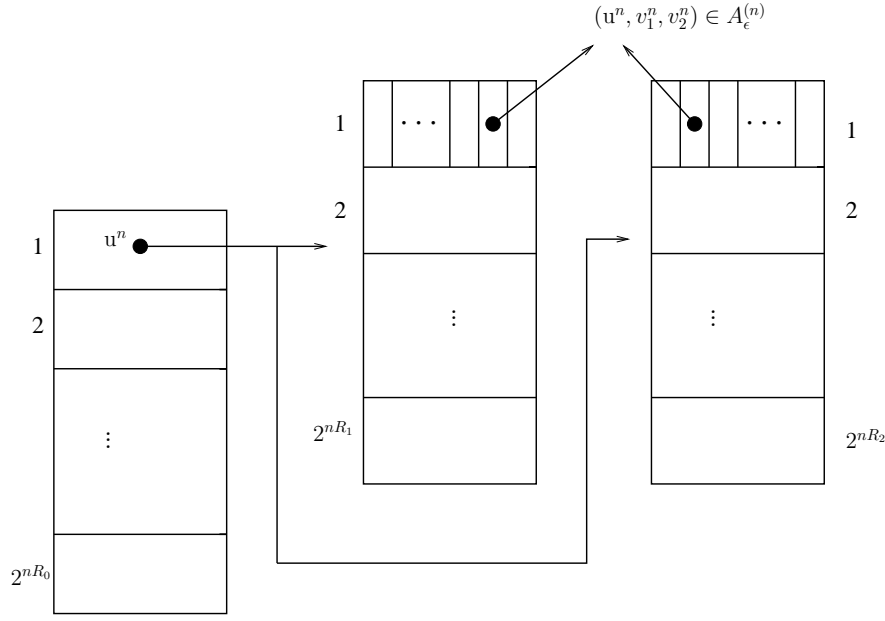


Fig. 7. The Stochastic Encoder

by i , for the codewords in each bin, randomly distribute them into $2^{nL_{12}}$ sub-bins indexed by i' ; thus i'' is the index for the codeword in each sub-bin. Similarly, for each codeword u^n , generate $2^{L_{21}+L_{22}+L_3}$ i.i.d codewords $v_2^n(j, j', j'')$ according to $P(v_2^n|u^n) = \prod_{i=1}^n P(v_{2i}|u_i)$, where $j \in \{1, 2, \dots, 2^{nL_{21}}\}$, $j' \in \{1, 2, \dots, 2^{nL_{22}}\}$ and $j'' \in \{1, 2, \dots, 2^{nL_3}\}$.

2) *Encoding*: To send messages (w_{10}, w_{20}, w_0) , we calculate the corresponding message index k and choose the corresponding codeword $u^n(k)$. Given this $u^n(k)$, there exists $2^{n(L_{11}+L_{12}+L_3)}$ codewords of $v_1^n(i, i', i'')$ to choose from for representing message w_{11} . Evenly map $2^{nR_{11}}$ messages w_{11} to $2^{nL_{11}}$ bins, then, given (27), each bin corresponds to at least one message w_{11} . Thus, given w_{11} , the bin index i can be decided.

- 1) If $R_{11} \leq L_{11} + L_{12}$, each bin corresponds to $2^{n(R_{11}-L_{11})}$ messages w_{11} . Evenly place the $2^{nL_{12}}$ sub-bins into $2^{n(R_{11}-L_{11})}$ cells. For each given w_{11} , we can find the corresponding cell, then, we randomly choose a sub-bin from that cell, thus the sub-bin index i' can be decided. The codeword $v_1^n(i, i', i'')$ will be chosen properly from that sub-bin.
- 2) If $L_{11} + L_{12} \leq R_{11} \leq L_{11} + L_{12} + L_3$, then each sub-bin is mapped to at least one message w_{11} , therefore, given w_{11} , i' can be decided. In each sub-bin, there are $2^{n(R_{11}-L_{11}-L_{12})}$ messages. The codeword $v_1^n(i, i', i'')$ will be chosen randomly and properly from that sub-bin.

Given w_{22} , we select $v_2^n(j, j', j'')$ in the exact same manner. From the given sub-bins, the encoder chooses the codeword pair $(v_1^n(i, i', i''), v_2^n(j, j', j''))$ that satisfies the following property,

$$(v_1^n(i, i', i''), v_2^n(j, j', j'')) \in A_\epsilon^{(n)}(V_1, V_2, U)$$

where $A_\epsilon^{(n)}(U, V_1, V_2)$ denotes the set of jointly typical sequences u^n , v_1^n , and v_2^n with respect to $P(u, v_1, v_2)$. If there is more than one such pair, the transmitter randomly chooses one; if there is no such pair, an error is declared.

Given v_1^n and v_2^n , the channel input x^n is generated i.i.d. according to the distribution $P(x^n|v_1^n, v_2^n) = \prod_{i=1}^n P(x_i|v_{1i}, v_{2i})$.

3) *Decoding*: The received signals at the legitimate receivers, y_1^n and y_2^n , are the outputs of the channels $P(y_1^n|x^n) = \prod_{i=1}^n P(y_{1i}|x_i)$ and $P(y_2^n|x^n) = \prod_{i=1}^n P(y_{2i}|x_i)$, respectively. The first receiver looks for the unique sequence $u^n(k)$ such that

$$(u^n(k), y_1^n) \in A_\epsilon^{(n)}(U, Y_1).$$

If such $u^n(k)$ exists and is unique, set $\hat{k} = k$; otherwise, declare an error. Upon decoding k , this receiver looks for sequences $v_1^n(i, i', i'')$ such that

$$(v_1^n(i, i', i''), u^n(k), y_1^n) \in A_\epsilon^{(n)}(V_1, U, Y_1).$$

If such $v_1^n(i, i', i'')$ exists and is unique, set $\hat{i} = i$, $\hat{i}' = i'$, and $\hat{i}'' = i''$; otherwise, declare an error. Using the values of \hat{k} , \hat{i} , \hat{i}' and \hat{i}'' , the decoder can calculate the message indices \hat{w}_0, \hat{w}_{10} and \hat{w}_{11} . The decoding for the second decoder is similar.

4) *Error Probability Analysis*: Since the region of \mathbb{R}_I is a subset of the Marton's region, then the error probability analysis is the same as [38].

5) *Equivocation Calculation*: To meet the secrecy requirements, we need to prove that the common message W_0 , the combination of (W_0, W_1) , the combination of (W_0, W_2) , and the combination of (W_0, W_1, W_2) are perfectly secured. The proof of secrecy requirement for the message W_0 is straightforward and is therefore omitted.

To prove the secrecy requirement for (W_0, W_1) , we have

$$\begin{aligned}
nR_{e10} &= H(W_1, W_0|Z^n) \\
&= H(W_1, W_0, Z^n) - H(Z^n) \\
&= H(W_1, W_0, U^n, V_1^n, Z^n) - H(U^n, V_1^n|W_1, W_0, Z^n) - H(Z^n) \\
&= H(W_1, W_0, U^n, V_1^n) + H(Z^n|W_1, W_0, U^n, V_1^n) - H(U^n|W_1, W_0, Z^n) - H(V_1^n|W_1, W_0, Z^n, U^n) - H(Z^n) \\
&\stackrel{(a)}{\geq} H(W_1, W_0, U^n, V_1^n) + H(Z^n|W_1, W_0, U^n, V_1^n) - n\epsilon_n - H(Z^n) \\
&\stackrel{(b)}{=} H(W_1, W_0, U^n, V_1^n) + H(Z^n|U^n, V_1^n) - n\epsilon_n - H(Z^n) \\
&\stackrel{(c)}{\geq} H(U^n, V_1^n) + H(Z^n|U^n, V_1^n) - n\epsilon_n - H(Z^n) \\
&= H(U^n) + H(V_1^n|U^n) - I(U^n, V_1^n; Z^n) - n\epsilon_n \\
&\stackrel{(d)}{\geq} \min\{I(U^n; Y_1^n), I(U^n; Y_2^n)\} + I(V_1^n; Y_1^n|U^n) - I(V_1^n; Z^n|U^n) - I(U^n; Z^n) - n\epsilon_n \\
&\stackrel{(e)}{\geq} nR_1 + nR_0 - n\epsilon_n,
\end{aligned}$$

where (a) follows from Fano's inequality that bounds the term $H(U^n|W_1, W_0, Z^n) \leq h(P_{we0}^{(n)}) + nP_{we0}^n R_{w0} \leq n\epsilon_n/2$ and the term $H(V_1^n|W_1, W_0, Z^n, U^n) \leq h(P_{we1}^{(n)}) + nP_{we1}^n R_{w1} \leq n\epsilon_n/2$ for sufficiently large n . Here P_{we0}^n and P_{we1}^n denotes the wiretapper's error probability of decoding u^n and V_1^n in the case that the bin numbers w_0 and w_1 are known to the eavesdropper, respectively. The eavesdropper first looks for the unique u^n in bin w_0 of the first layer, such that it is jointly typical with z^n . As the number of candidate codewords is small enough, the probability of error is arbitrarily small for a sufficiently large n . Next, given u^n , the eavesdropper looks for the unique v_1^n in the bin w_1 which is jointly typical with z^n . Similarly, since the number of available candidates is small enough, then the probability of decoding error is arbitrarily small. (b) follows from the fact that $(W_1, W_0) \rightarrow U^n \rightarrow V_1^n \rightarrow Z^n$ forms a Markov chain. Therefore, we have $I(W_1, W_0; Z^n|U^n, V_1^n) = 0$, where it is implied that $H(Z^n|W_1, W_0, U^n, V_1^n) = H(Z^n|U^n, V_1^n)$. (c) follows from the fact that $H(W_1, W_0, U^n, X^n) \geq H(U^n, X^n)$. (d) follows from that fact that $H(U^n) \geq \min\{I(U^n; Y_1^n), I(U^n; Y_2^n)\}$ and $H(V_1^n|U^n) \geq I(V_1^n; Y_1^n|U^n)$. (e) follows from Lemma 4 of the appendix IV.

By using the same approach it is easy to show that,

$$\begin{aligned}
nR_{e20} &= H(W_2, W_0|Z^n) \\
&\geq nR_2 + nR_0 - n\epsilon_n.
\end{aligned}$$

Therefore, we only need to prove that (W_0, W_1, W_2) is perfectly secured; we have

$$\begin{aligned}
nR_{e120} &= H(W_1, W_2, W_0|Z^n) \\
&= H(W_1, W_2, W_0, Z^n) - H(Z^n) \\
&= H(W_1, W_2, W_0, U^n, V_1^n, V_2^n, Z^n) - H(U^n, V_1^n, V_2^n|W_1, W_2, W_0, Z^n) - H(Z^n) \\
&= H(W_1, W_2, W_0, U^n, V_1^n, V_2^n) + H(Z^n|W_1, W_2, W_0, U^n, V_1^n, V_2^n) - H(U^n, V_1^n, V_2^n|W_1, W_2, W_0, Z^n) \\
&\quad - H(Z^n) \\
&\stackrel{(a)}{\geq} H(W_1, W_2, W_0, U^n, V_1^n, V_2^n) + H(Z^n|W_1, W_2, W_0, U^n, V_1^n, V_2^n) - n\epsilon_n - H(Z^n) \\
&\stackrel{(b)}{=} H(W_1, W_2, W_0, U^n, V_1^n, V_2^n) + H(Z^n|U^n, V_1^n, V_2^n) - n\epsilon_n - H(Z^n) \\
&\stackrel{(c)}{\geq} H(U^n, V_1^n, V_2^n) + H(Z^n|U^n, V_1^n, V_2^n) - n\epsilon_n - H(Z^n) \\
&\stackrel{(d)}{=} H(U^n) + H(V_1^n|U^n) + H(V_2^n|U^n) - I(V_1^n; V_2^n|U^n) + H(Z^n|U^n, V_1^n, V_2^n) - n\epsilon_n - H(Z^n) \\
&\stackrel{(e)}{\geq} \min\{I(U^n; Y_1^n), I(U^n; Y_2^n)\} + I(V_1^n; Y_1^n|U^n) + I(V_2^n; Y_2^n|U^n) - I(V_1^n; V_2^n|U^n) - I(U^n, V_1^n, V_2^n; Z^n) \\
&\quad - n\epsilon_n \\
&\stackrel{(f)}{\geq} \min\{I(U^n; Y_1^n), I(U^n; Y_2^n)\} + I(V_1^n; Y_1^n|U^n) + I(V_2^n; Y_2^n|U^n) - I(V_1^n; V_2^n|U^n) - I(V_1^n, V_2^n; Z^n|U^n) \\
&\quad - I(U^n; Z^n) - n\epsilon_n \\
&\stackrel{(g)}{\geq} n \min\{I(U; Y_1), I(U; Y_2)\} + nI(V_1; Y_1|U) + nI(V_2; Y_2|U) - nI(V_1; V_2|U) - nI(V_1, V_2; Z|U) \\
&\quad - nI(U; Z) - n\epsilon_n \\
&\geq nR_1 + nR_2 + nR_0 - n\epsilon_n,
\end{aligned}$$

where (a) follows from Fano's inequality, which states that for sufficiently large n , $H(U^n, V_1^n, V_2^n|W_1, W_2, W_0, Z^n) \leq h(P_{we}^{(n)}) + nP_{we}^{(n)}R_w \leq n\epsilon_n$. Here $P_{we}^{(n)}$ denotes the wiretapper's error probability of decoding (u^n, v_1^n, v_2^n) in the case that the bin numbers w_0, w_1 , and w_2 are known to the eavesdropper. Since the sum rate is small enough, then $P_{we}^{(n)} \rightarrow 0$ for sufficiently large n . (b) follows from the following Markov chain: $(W_1, W_2, W_0) \rightarrow (U^n, V_1^n, V_2^n) \rightarrow Z^n$. Hence, we have $H(Z^n|W_1, W_2, W_0, U^n, V_1^n, V_2^n) = H(Z^n|U^n, V_1^n, V_2^n)$. (c) follows from the fact that $H(W_1, W_2, W_0, U^n, V_1^n, V_2^n) \geq H(U^n, V_1^n, V_2^n)$. (d) follows from that fact that $H(U^n, V_1^n, V_2^n) = H(U^n) + H(V_1^n|U^n) + H(V_2^n|U^n) - I(V_1^n; V_2^n|U^n)$. (e) follows from the fact that $H(U^n) \geq \min\{I(U^n; Y_1^n), I(U^n; Y_2^n)\}$ and $H(V_i^n|U^n) \geq I(V_i^n; Y_i^n|U^n)$ for $i = 1, 2$. (f) follows from the fact that $I(U^n, V_1^n, V_2^n; Z^n) = I(U^n; Z^n) + I(V_1^n, V_2^n; Z^n|U^n)$. (g) follows from Lemma 3 and Lemma 4 in the appendix IV. This completes the achievability proof.

APPENDIX II PROOF OF THEOREM 2

Achievability: We need to show that the region of (13) and (14) is a subset of the achievability region of Theorem 1. In the achievability scheme of Theorem 1, if we set $\mathcal{W}_2 = \emptyset$ and rename W_0 with W_2 , then using the degradedness, we obtain the following region,

$$\begin{aligned}
R_1 + R_2 &\leq I(V; Y_1|U) - I(V; Z|U) + I(U; Y_2) - I(U; Z), \\
R_2 &\leq I(U; Y_2) - I(U; Z).
\end{aligned} \tag{29}$$

Note that since the first receiver decodes both messages, the total rate of this receiver is $R_1 \leftarrow R_1 + R_2$ and we have

$$\begin{aligned}
R_1 &\leq I(UV; Y_1|U) + I(U; Y_2) - I(UV; Z), \\
R_2 &\leq I(U; Y_2) - I(U; Z).
\end{aligned} \tag{30}$$

Now, since $U \rightarrow V \rightarrow X \rightarrow Y_2 \rightarrow Z$ is a markov chain, then the following region is a subset of the above region, and consequently, it is achievable,

$$\begin{aligned}
R_1 &\leq I(X; Y_1|U) + I(U; Z) - I(X; Z), \\
R_2 &\leq I(U; Y_2) - I(U; Z).
\end{aligned} \tag{31}$$

which is the same as that of region (13) and (14). This completes the achievability proof.

Converse: The transmitter sends two independent secret messages W_1 and W_2 to Receiver 1 and Receiver 2, respectively. Let us define $U_i = (W_2, Y_1^{i-1})$. The following Lemma bounds the secrecy rates for a general case of $(W_1, W_2) \rightarrow X^n \rightarrow Y_1^n Y_2^n Z^n$:

Lemma 2 For the broadcast channel with an eavesdropper, the perfect secrecy rates are bounded as follows,

$$\begin{aligned} nR_1 &\leq \sum_{i=1}^n I(W_1; Y_{1i} | W_2, Z_i, Y_1^{i-1}, \tilde{Z}^{i+1}) + n\delta_1 + n\epsilon_3, \\ nR_2 &\leq \sum_{i=1}^n I(W_2; Y_{2i} | Z_i, Y_2^{i-1}, \tilde{Z}^{i+1}) + n\delta_1 + n\epsilon_2. \end{aligned}$$

Proof: We need to prove the second bound. The first bound can similarly be proven. nR_2 is bounded as follows:

$$\begin{aligned} nR_2 &\stackrel{(a)}{\leq} H(W_2 | Z^n) + n\epsilon_2 \\ &\stackrel{(b)}{\leq} H(W_2 | Z^n) - H(W_2 | Y_2^n) + n\delta_1 + n\epsilon_2 \\ &= I(W_2; Y_2^n) - I(W_2; Z^n) + n\delta_1 + n\epsilon_2 \end{aligned}$$

where (a) follows from the secrecy constraint that $H(W_2 | Z^n) \geq H(W_2) - n\epsilon_2$. (b) follows from Fano's inequality that $H(W_2 | Y_2^n) \leq n\delta_1$. Next, we expand $I(W_2; Y_2^n)$ and $I(W_2; Z^n)$ as follows.

$$\begin{aligned} I(W_2; Y_2^n) &= \sum_{i=1}^n I(W_2; Y_{2i} | Y_2^{i-1}) \\ &= \sum_{i=1}^n I(W_2, \tilde{Z}^{i+1}; Y_{2i} | Y_2^{i-1}) - I(\tilde{Z}^{i+1}; Y_{2i} | W_2, Y_2^{i-1}) \\ &= \sum_{i=1}^n I(W_2; Y_{2i} | Y_2^{i-1}, \tilde{Z}^{i+1}) + I(\tilde{Z}^{i+1}; Y_{2i} | Y_2^{i-1}) - I(\tilde{Z}^{i+1}; Y_{2i} | W_2, Y_2^{i-1}) \\ &= \sum_{i=1}^n I(W_2; Y_{2i} | Y_2^{i-1}, \tilde{Z}^{i+1}) + \Delta_1 - \Delta_2, \end{aligned}$$

where, $\Delta_1 = \sum_{i=1}^n I(\tilde{Z}^{i+1}; Y_{2i} | Y_2^{i-1})$ and $\Delta_2 = \sum_{i=1}^n I(\tilde{Z}^{i+1}; Y_{2i} | W_2, Y_2^{i-1})$. Similarly, we have,

$$\begin{aligned} I(W_2; Z^n) &= \sum_{i=1}^n I(W_2; Z_i | \tilde{Z}^{i+1}) \\ &= \sum_{i=1}^n I(W_2, Y_2^{i-1}; Z_i | \tilde{Z}^{i+1}) - I(Y_2^{i-1}; Z_i | W_2, \tilde{Z}^{i+1}) \\ &= \sum_{i=1}^n I(W_2; Z_i | Y_2^{i-1}, \tilde{Z}^{i+1}) + I(Y_2^{i-1}; Z_i | \tilde{Z}^{i+1}) - I(Y_2^{i-1}; Z_i | W_2, \tilde{Z}^{i+1}) \\ &= \sum_{i=1}^n I(W_2; Z_i | Y_2^{i-1}, \tilde{Z}^{i+1}) + \Delta_1^* - \Delta_2^*, \end{aligned}$$

where, $\Delta_1^* = \sum_{i=1}^n I(Y_2^{i-1}; Z_i | \tilde{Z}^{i+1})$ and $\Delta_2^* = \sum_{i=1}^n I(Y_2^{i-1}; Z_i | W_2, \tilde{Z}^{i+1})$. According to Lemma 7 of [4], $\Delta_1 = \Delta_1^*$ and $\Delta_2 = \Delta_2^*$. Thus, we have,

$$\begin{aligned} nR_2 &\leq \sum_{i=1}^n I(W_2; Y_{2i} | Y_2^{i-1}, \tilde{Z}^{i+1}) - I(W_2; Z_i | Y_2^{i-1}, \tilde{Z}^{i+1}) + n\delta_1 + n\epsilon_2 \\ &= \sum_{i=1}^n H(W_2 | Z_i, Y_2^{i-1}, \tilde{Z}^{i+1}) - H(W_2 | Y_{2i}, Y_2^{i-1}, \tilde{Z}^{i+1}) + n\delta_1 + n\epsilon_2 \\ &\stackrel{(a)}{\leq} \sum_{i=1}^n H(W_2 | Z_i, Y_2^{i-1}, \tilde{Z}^{i+1}) - H(W_2 | Y_{2i}, Z_i, Y_2^{i-1}, \tilde{Z}^{i+1}) + n\delta_1 + n\epsilon_2 \\ &= \sum_{i=1}^n I(W_2; Y_{2i} | Z_i, Y_2^{i-1}, \tilde{Z}^{i+1}) + n\delta_1 + n\epsilon_2, \end{aligned}$$

where (a) follows from the fact that conditioning always decreases the entropy. ■

Now according to the above Lemma, the secrecy rates are bounded as follows:

$$\begin{aligned}
nR_1 &\stackrel{(a)}{\leq} \sum_{i=1}^n I(W_1; Y_{1,i} | W_2, Z_i, Y_1^{i-1}, \tilde{Z}^{i+1}) + n\delta_1 + n\epsilon_3 \\
&= \sum_{i=1}^n I(W_1; Y_{1,i} | U_i, Z_i, \tilde{Z}^{i+1}) + n\delta_1 + n\epsilon_3 \\
&\stackrel{(b)}{\leq} \sum_{i=1}^n I(X_i; Y_{1,i} | U_i, Z_i, \tilde{Z}^{i+1}) + n\delta_1 + n\epsilon_3 \\
&\stackrel{(c)}{=} \sum_{i=1}^n I(X_i; Y_{1,i}, U_i, Z_i | \tilde{Z}^{i+1}) - I(X_i; Z_i | \tilde{Z}^{i+1}) - I(X_i; U_i | Z_i, \tilde{Z}^{i+1}) + n\delta_1 + n\epsilon_3 \\
&\stackrel{(d)}{=} \sum_{i=1}^n I(X_i; Y_{1,i} | U_i, \tilde{Z}^{i+1}) + I(X_i; U_i | \tilde{Z}^{i+1}) - I(X_i; Z_i | \tilde{Z}^{i+1}) - I(X_i; U_i | Z_i, \tilde{Z}^{i+1}) + n\delta_1 + n\epsilon_3 \\
&\stackrel{(e)}{=} \sum_{i=1}^n I(X_i; Y_{1,i} | U_i, \tilde{Z}^{i+1}) - I(X_i; Z_i | \tilde{Z}^{i+1}) + I(Z_i; U_i | \tilde{Z}^{i+1}) - I(Z_i; U_i | X_i, \tilde{Z}^{i+1}) + n\delta_1 + n\epsilon_3 \\
&\stackrel{(f)}{=} \sum_{i=1}^n I(X_i; Y_{1,i} | U_i, \tilde{Z}^{i+1}) - I(X_i; Z_i | \tilde{Z}^{i+1}) + I(Z_i; U_i | \tilde{Z}^{i+1}) + n\delta_1 + n\epsilon_3,
\end{aligned}$$

where (a) follows from the Lemma (2). (b) follows from the data processing theorem. (c) follows from the chain rule. (d) follows from the fact that $I(X_i; Y_{1,i}, U_i, Z_i | \tilde{Z}^{i+1}) = I(X_i; U_i | \tilde{Z}^{i+1}) + I(X_i; Y_{1,i} | U_i, \tilde{Z}^{i+1}) + I(X_i; Z_i | Y_{1,i}, U_i, \tilde{Z}^{i+1})$ and from the fact that $\tilde{Z}^{i+1} U_i \rightarrow X_i \rightarrow Y_{1,i} \rightarrow Y_{2,i} \rightarrow Z_i$ forms a Markov chain, which means that $I(X_i; Z_i | Y_{1,i}, U_i, \tilde{Z}^{i+1}) = 0$. (e) follows from the fact that $I(X_i; U_i | \tilde{Z}^{i+1}) - I(X_i; U_i | Z_i, \tilde{Z}^{i+1}) = I(Z_i; U_i | \tilde{Z}^{i+1}) - I(Z_i; U_i | X_i, \tilde{Z}^{i+1})$. (f) follows from the fact that $\tilde{Z}^{i+1} U_i \rightarrow X_i \rightarrow Z_i$ forms a Markov chain. Thus, $I(Z_i; U_i | \tilde{Z}^{i+1} X_i) = 0$ which implies that $I(Z_i; U_i | X_i, \tilde{Z}^{i+1}) = 0$.

For the second receiver, we have

$$\begin{aligned}
nR_2 &\stackrel{(a)}{\leq} \sum_{i=1}^n I(W_2; Y_{2,i} | Y_2^{i-1}, Z_i, \tilde{Z}^{i+1}) + n\delta_2 + n\epsilon_1 \\
&= \sum_{i=1}^n H(Y_{2,i} | Y_2^{i-1}, Z_i, \tilde{Z}^{i+1}) - H(Y_{2,i} | W_2, Y_2^{i-1}, Z_i, \tilde{Z}^{i+1}) + n\delta_2 + n\epsilon_1 \\
&\stackrel{(b)}{\leq} \sum_{i=1}^n H(Y_{2,i} | Z_i, \tilde{Z}^{i+1}) - H(Y_{2,i} | W_2, Y_1^{i-1}, Y_2^{i-1}, Z_i, \tilde{Z}^{i+1}) + n\delta_2 + n\epsilon_1 \\
&\stackrel{(c)}{=} \sum_{i=1}^n H(Y_{2,i} | Z_i, \tilde{Z}^{i+1}) - H(Y_{2,i} | U_i, Z_i, \tilde{Z}^{i+1}) + n\delta_2 + n\epsilon_1 \\
&= \sum_{i=1}^n I(Y_{2,i}; U_i | Z_i, \tilde{Z}^{i+1}) + n\delta_2 + n\epsilon_1 \\
&= \sum_{i=1}^n I(Y_{2,i}; U_i | \tilde{Z}^{i+1}) + I(Y_{2,i}; Z_i | U_i, \tilde{Z}^{i+1}) - I(Y_{2,i}; Z_i | \tilde{Z}^{i+1}) + n\delta_2 + n\epsilon_1 \\
&= \sum_{i=1}^n I(Y_{2,i}; U_i | \tilde{Z}^{i+1}) - I(Z_i; U_i | \tilde{Z}^{i+1}) + I(Z_i; U_i | Y_{2,i}, \tilde{Z}^{i+1}) + n\delta_2 + n\epsilon_1 \\
&\stackrel{(d)}{=} \sum_{i=1}^n I(Y_{2,i}; U_i | \tilde{Z}^{i+1}) - I(Z_i; U_i | \tilde{Z}^{i+1}) + n\delta_2 + n\epsilon_1,
\end{aligned}$$

where (a) follows from the lemma (2). (b) follows from the fact that conditioning always decreases the entropy. (c) follows from the fact that $Y_2^{i-1} \rightarrow W_2 \tilde{Z}^{i+1} Y_1^{i-1} \rightarrow Y_{2,i} \rightarrow Z_i$ forms a Markov chain. (d) follows from the fact that $\tilde{Z}^{i+1} U_i \rightarrow Y_{2,i} \rightarrow Z_i$ forms a Markov chain. Thus $I(Z_i; U_i | \tilde{Z}^{i+1} Y_{2,i}) = 0$ which implies that $I(Z_i; U_i | Y_{2,i}, \tilde{Z}^{i+1}) = 0$. Now, following [39], let us define the time sharing random variable Q which is uniformly distributed over $\{1, 2, \dots, n\}$ and independent of $(W_1, W_2, X^n, Y_1^n, Y_2^n)$. Let us define $U = U_Q$, $V = (\tilde{Z}^{Q+1}, Q)$, $X = X_Q$, $Y_1 = Y_{1,Q}$, $Y_2 = Y_{2,Q}$, $Z = Z_Q$, then R_1 and R_2 can be written as

$$R_1 \leq I(X; Y_1 | U, V) + I(U; Z | V) - I(X; Z | V), \quad (32)$$

$$R_2 \leq I(U; Y_2 | V) - I(U; Z | V). \quad (33)$$

Note that the boundary of this region is characterized by the maximization of $R_1 + \mu R_2$ over this region for $\mu \geq 1$. On the other hand we have,

$$R_1 + \mu R_2 \leq I(X; Y_1|U, V) + I(U; Z|V) - I(X; Z|V) + \mu (I(U; Y_2|V) - I(U; Z|V)) \quad (34)$$

Since conditional mutual information is the average of the unconditional ones, the largest region is achieved when V is a constant. This proves the converse part.

APPENDIX III PROOF OF THEOREM 3

Achievability: Let $U \sim \mathcal{N}(0, (1 - \alpha)P)$ and $X' \sim \mathcal{N}(0, \alpha P)$ be independent and $X = U + X' \sim \mathcal{N}(0, P)$. Now consider the following secure superposition coding scheme:

1) *Codebook Generation:* Generate $2^{nI(U; Y_2)}$ i.i.d Gaussian codewords u^n with average power $(1 - \alpha)P$ and randomly distribute these codewords into 2^{nR_2} bins. Then index each bin by $w_2 \in \{1, 2, \dots, 2^{nR_2}\}$. Generate an independent set of $2^{nI(X'; Y_1)}$ i.i.d Gaussian codewords x'^n with average power αP . Then, randomly distribute them into 2^{nR_1} bins. Index each bin by $w_1 \in \{1, 2, \dots, 2^{nR_1}\}$.

2) *Encoding:* To send messages w_1 and w_2 , the transmitter randomly chooses one of the codewords in bin w_2 , (say u^n) and one of the codewords in bin w_1 (say x'^n). The transmitter then simply transmits $x^n = u^n + x'^n$.

3) *Decoding:* The received signal at the legitimate receivers are y_1^n and y_2^n , respectively. Receiver 2 determines the unique u^n such that (u^n, y_2^n) are jointly typical and declares the index of the bin containing u^n as the message received. If there is none of such or more than one of such, an error is declared. Receiver 1 uses the successive cancellation method; it first decodes u^n and subtracts it from y_1^n and then looks for the unique x'^n such that $(x'^n, y_1^n - u^n)$ are jointly typical and declares the index of the bin containing x'^n as the message received.

It can be shown that if R_1 and R_2 satisfy (15) and (16), the error probability analysis and equivocation calculation is straightforward and may therefore be omitted.

Converse: According to the previous section, R_2 is bounded as follows:

$$nR_2 \leq I(Y_2^n; U^n|Z^n) = h(Y_2^n|Z^n) - h(Y_2^n|U^n, Z^n), \quad (35)$$

where h is the differential entropy. The classical entropy power inequality states that:

$$2^{\frac{2}{n}h(Y_2^n + N_3'^n)} \geq 2^{\frac{2}{n}h(Y_2^n)} + 2^{\frac{2}{n}h(N_3'^n)}$$

Therefore, $h(Y_2^n|Z^n)$ may be written as follows:

$$\begin{aligned} h(Y_2^n|Z^n) &= h(Z^n|Y_2^n) + h(Y_2^n) - h(Z^n) \\ &= \frac{n}{2} \log 2\pi e(\sigma_3^2 - \sigma_2^2) + h(Y_2^n) - h(Y_2^n + N_3'^n) \\ &\leq \frac{n}{2} \log 2\pi e(\sigma_3^2 - \sigma_2^2) + h(Y_2^n) - \frac{n}{2} \log(2^{\frac{2}{n}h(Y_2^n)} + 2\pi e(\sigma_3^2 - \sigma_2^2)). \end{aligned}$$

On the other hand, for any fixed $a \in \mathcal{R}$, the function

$$f(t, a) = t - \frac{n}{2} \log(2^{\frac{2}{n}t} + a)$$

is concave in t and has a global maximum at the maximum value of t . Thus, $h(Y_2^n|Z^n)$ is maximized when Y_2^n (or equivalently X^n) has Gaussian distribution. Hence,

$$\begin{aligned} h(Y_2^n|Z^n) &\leq \frac{n}{2} \log 2\pi e(\sigma_3^2 - \sigma_2^2) + \frac{n}{2} \log 2\pi e(P + \sigma_2^2) - \frac{n}{2} \log 2\pi e(P + \sigma_3^2) \\ &= \frac{n}{2} \log \left(\frac{2\pi e(\sigma_3^2 - \sigma_2^2)(P + \sigma_2^2)}{P + \sigma_3^2} \right). \end{aligned} \quad (36)$$

Note that another method to obtain (36) is using the worst additive noise lemma (see [46], [47] for details). Now consider the term $h(Y_2^n|U^n, Z^n)$. This term is lower bounded with $h(Y_2^n|U^n, X^n, Z^n) = \frac{n}{2} \log 2\pi e(\sigma_2^2)$ which is greater than $\frac{n}{2} \log 2\pi e(\frac{\sigma_2^2(\sigma_3^2 - \sigma_2^2)}{\sigma_3^2})$. Hence,

$$\frac{n}{2} \log 2\pi e(\frac{\sigma_2^2(\sigma_3^2 - \sigma_2^2)}{\sigma_3^2}) \leq h(Y_2^n|U^n, Z^n) \leq h(Y_2^n|Z^n). \quad (37)$$

Inequalities (36) and (37) imply that there exists an $\alpha \in [0, 1]$ such that

$$h(Y_2^n|U^n, Z^n) = \frac{n}{2} \log \left(\frac{2\pi e(\sigma_3^2 - \sigma_2^2)(\alpha P + \sigma_2^2)}{\alpha P + \sigma_3^2} \right). \quad (38)$$

Substituting (38) and (36) into (35) yields the desired bound

$$\begin{aligned}
nR_2 &\leq h(Y_2^n|Z^n) - h(Y_2^n|U^n, Z^n) \\
&\leq \frac{n}{2} \log \left(\frac{(P + \sigma_2^2)(\alpha P + \sigma_3^2)}{(P + \sigma_3^2)(\alpha P + \sigma_2^2)} \right) \\
&= nC \left(\frac{(1 - \alpha)P}{\alpha P + \sigma_2^2} \right) - nC \left(\frac{(1 - \alpha)P}{\alpha P + \sigma_3^2} \right).
\end{aligned} \tag{39}$$

Note that the left hand side of (38) can be written as $h(Y_2^n, Z^n|U^n) - h(Z^n|U^n)$ which implies that

$$h(Y_2^n|U^n) - h(Z^n|U^n) = \frac{n}{2} \log \left(\frac{\alpha P + \sigma_2^2}{\alpha P + \sigma_3^2} \right). \tag{40}$$

Since $\sigma_1^2 \leq \sigma_2^2 \leq \sigma_3^2$, there exists a $0 \leq \beta \leq 1$ such that $\sigma_2^2 = (1 - \beta)\sigma_1^2 + \beta\sigma_3^2$, or equivalently, $\sigma_2^2 = \sigma_1^2 + \beta(\sigma_3^2 - \sigma_1^2)$. Therefore, since $Y_1^n \rightarrow Y_2^n \rightarrow Z^n$ forms a Markov chain, the received signals Z^n and Y_2^n can be written as $Z^n = Y_1^n + \tilde{N}^n$ and $Y_2^n = Y_1^n + \sqrt{\beta}\tilde{N}^n$ where \tilde{N} is an independent Gaussian noise with variance $\tilde{\sigma}^2 = \sigma_3^2 - \sigma_1^2$. All noises are Gaussian random n -vector with a positive definite covariance matrix. Costa's entropy power inequality [48] states that (see also [49] for its linear version),

$$2^{\frac{2}{n}h(Y_1^n + \sqrt{\beta}\tilde{N}^n|U^n)} \geq (1 - \beta)2^{\frac{2}{n}h(Y_1^n|U^n)} + \beta 2^{\frac{2}{n}h(Y_1^n + \tilde{N}^n|U^n)} \tag{41}$$

for any random n -vector Y_1^n and Gaussian random n -vector of \tilde{N}^n . Equivalently we have,

$$2^{\frac{2}{n}h(Y_2^n|U^n)} \geq (1 - \beta)2^{\frac{2}{n}h(Y_1^n|U^n)} + \beta 2^{\frac{2}{n}h(Z^n|U^n)} \tag{42}$$

After some manipulations of (42), we obtain

$$\begin{aligned}
&h(Y_1^n|U^n) - h(Z^n|U^n) \\
&\leq \frac{n}{2} \log \left(\frac{\alpha P + \sigma_2^2 - \beta(\alpha P + \sigma_3^2)}{(1 - \beta)(\alpha P + \sigma_3^2)} \right) \\
&= \frac{n}{2} \log \left(\frac{\alpha P + \sigma_1^2}{\alpha P + \sigma_3^2} \right).
\end{aligned} \tag{43}$$

The rate R_1 is bounded as follows

$$\begin{aligned}
nR_1 &\leq I(X^n; Y_1^n|U^n) - I(X^n; Z^n) + I(U^n; Z^n) \\
&= h(Y_1^n|U^n) - h(Y_1^n|X^n, U^n) + h(Z^n|X^n) - h(Z^n|U^n) \\
&= h(Y_1^n|U^n) - h(Z^n|U^n) + \frac{n}{2} \log \left(\frac{\sigma_3^2}{\sigma_1^2} \right) \\
&\stackrel{(a)}{\leq} \frac{n}{2} \log \left(\frac{\alpha P + \sigma_1^2 \sigma_3^2}{\alpha P + \sigma_3^2 \sigma_1^2} \right) \\
&= nC \left(\frac{\alpha P}{\sigma_1^2} \right) - nC \left(\frac{\alpha P}{\sigma_3^2} \right),
\end{aligned} \tag{44}$$

where (a) follows from (43).

APPENDIX IV COMPLEMENTARY LEMMAS FOR EQUIVOCATION ANALYSIS

Lemma 3 Assume U^n, V_1^n, V_2^n and Z^n are generated according to the achievability scheme of Theorem 1, then we have,

$$\begin{aligned}
I(V_1^n, V_2^n; Z^n|U^n) &\leq nI(V_1, V_2; Z|U) + n\delta_{1n}, \\
I(V_1^n; V_2^n|U^n) &\leq nI(V_1; V_2|U) + n\delta_{2n}.
\end{aligned}$$

Proof: Let $A_\epsilon^n(P_{U, V_1, V_2, Z})$ denote the set of typical sequences (U^n, V_1^n, V_2^n, Z^n) with respect to $P_{U, V_1, V_2, Z}$, and

$$\zeta = \begin{cases} 1, & (U^n, V_1^n, V_2^n, Z^n) \notin A_\epsilon^n(P_{U, V_1, V_2, Z}); \\ 0, & \text{otherwise,} \end{cases}$$

be the corresponding indicator function. We expand $I(V_1^n, V_2^n; Z^n|U^n)$ as follow,

$$\begin{aligned}
I(V_1^n, V_2^n; Z^n|U^n) &\leq I(V_1^n, V_2^n, \zeta; Z^n|U^n) \\
&= I(V_1^n, V_2^n; Z^n|U^n, \zeta) + I(\zeta; Z^n|U^n) \\
&= \sum_{j=0}^1 P(\zeta = j) I(V_1^n, V_2^n; Z^n|U^n, \zeta = j) + I(\zeta; Z^n|U^n).
\end{aligned} \tag{45}$$

According to the joint typicality property, we have

$$\begin{aligned} P(\zeta = 1)I(V_1^n, V_2^n; Z^n|U^n, \zeta = 1) &\leq nP((U^n, V_1^n, V_2^n, Z^n) \notin A_\epsilon^n(P_{U, V_1, V_2, Z})) \log \|\mathcal{Z}\| \\ &\leq n\epsilon_n \log \|\mathcal{Z}\|. \end{aligned} \quad (46)$$

Note that,

$$I(\zeta; Z^n|U^n) \leq H(\zeta) \leq 1 \quad (47)$$

Now consider the term $P(\zeta = 0)I(V_1^n, V_2^n; Z^n|U^n, \zeta = 0)$. Following the sequence joint typicality properties, we have

$$\begin{aligned} P(\zeta = 0)I(V_1^n, V_2^n; Z^n|U^n, \zeta = 0) &\leq I(V_1^n, V_2^n; Z^n|U^n, \zeta = 0) \\ &= \sum_{(U^n, V_1^n, V_2^n, Z^n) \in A_\epsilon^n} P(U^n, V_1^n, V_2^n, Z^n) (\log P(V_1^n, V_2^n, Z^n|U^n) - \log P(V_1^n, V_2^n|U^n) \\ &\quad - \log P(Z^n|U^n)), \\ &\leq n[-H(V_1, V_2, Z|U) + H(V_1, V_2|U) + H(Z|U) + 3\epsilon_n], \\ &= n[I(V_1, V_2; Z|U) + 3\epsilon_n]. \end{aligned} \quad (48)$$

By substituting (46), (47), and (48) into (45), we get the desired result,

$$\begin{aligned} I(V_1^n, V_2^n; Z^n|U^n) &\leq nI(V_1, V_2; Z|U) + n\left(\epsilon_n \log \|\mathcal{Z}\| + 3\epsilon_n + \frac{1}{n}\right), \\ &= nI(V_1, V_2; Z|U) + n\delta_{1n}, \end{aligned} \quad (49)$$

where,

$$\delta_{1n} = \epsilon_n \log \|\mathcal{Z}\| + 3\epsilon_n + \frac{1}{n}.$$

Following the same steps, one can prove that

$$I(V_1^n; V_2^n|U^n) \leq nI(V_1; V_2|U) + n\delta_{2n}. \quad (50)$$

■

Using the same approach as in Lemma 3, we can prove the following lemmas.

Lemma 4 Assume U^n, V_1^n, Y_1^n and Y_2^n are generated according to the achievability scheme of Theorem 1, then we have,

$$\begin{aligned} I(V_1^n; Y_1^n|U^n) &\leq nI(V_1; Y_1|U) + n\delta_{3n}, \\ I(V_1^n; Z^n|U^n) &\leq nI(V_1; Z|U) + n\delta_{4n}, \\ I(U^n; Z^n) &\leq nI(U; Z) + n\delta_{5n}, \\ I(U^n; Y_1^n) &\leq nI(U; Y_1) + n\delta_{6n}, \\ I(U^n; Y_2^n) &\leq nI(U; Y_2) + n\delta_{7n}. \end{aligned}$$

Proof: The steps of the proof are very similar to the steps of proof of Lemma 3 and may be omitted here. ■

REFERENCES

- [1] C. E. Shannon, "Communication Theory of Secrecy Systems", *Bell System Technical Journal*, vol. 28, pp. 656-715, Oct. 1949.
- [2] A. Wyner, "The Wire-tap Channel", *Bell System Technical Journal*, vol. 54, pp. 1355-1387, 1975.
- [3] S. K. Leung-Yan-Cheong and M. E. Hellman, "Gaussian Wiretap Channel", *IEEE Trans. Inform. Theory*, vol. 24, no. 4, pp. 451-456, July 1978.
- [4] I. Csiszar and J. Korner, "Broadcast Channels with Confidential Messages", *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339-348, May 1978.
- [5] R. Liu, I. Maric, P. Spasojevic and R. D. Yates, "Discrete Memoryless Interference and Broadcast Channels with Confidential Messages", *IEEE Trans. Inform. Theory*, Vol. 54, Issue: 6, pp. 2493-2507, Jun 2008.
- [6] J. Xu and B. Chen, "Broadcast Confidential and Public Messages", in *Proc. 42nd Conf. Information Sciences and Systems (CISS)*, Princeton, NJ, pp. 630-635 Mar. 2008.
- [7] J. Xu, Y. Cao, and B. Chen, "Capacity Bounds for Broadcast Channels with Confidential Messages", *IEEE Trans. Inform. Theory*, Volume 55, Issue 10, pp. 4529 - 4542, Oct. 2009.
- [8] P. K. Gopala, L. Lai and H. El-Gamal, "On the Secrecy Capacity of Fading Channels", in *IEEE Trans. on Info. Theory*, Volume 54, Issue 10, pp. 4687-4698, Oct. 2008.
- [9] P. Parada and R. Blahut, "Secrecy Capacity of SIMO and Slow Fading Channels," in *Proc. of ISIT 2005*, pp. 2152-2155, Sep. 2005.
- [10] J. Barros and M. R. D. Rodrigues, "Secrecy Capacity of Wireless Channels", in *Proc. of ISIT 2006*, pp. 356-360, July 2006.
- [11] S. Shamai, A. Steiner, "A Broadcast Approach for a Single-User Slowly Fading MIMO Channel", in *IEEE Trans. on Info. Theory*, Volume 49, Issue 10, pp. 2617-2635, Oct. 2003.
- [12] S. Shamai, "A Broadcast Strategy for the Gaussian Slowly Fading Channel", in *IEEE International Symposium on Info. Theory*, pp. 150, July 1997.
- [13] A. Steiner, S. Shamai, "Single-User Broadcasting Protocols Over a Two-Hop Relay Fading Channel", in *IEEE Trans. on Info. Theory*, Volume 52, Issue 11, pp. 4821-4838, Nov. 2006.
- [14] A. Steiner, S. Shamai, "Multi-Layer Broadcasting Hybrid-ARQ Strategies for Block Fading Channels", in *IEEE Trans. on Wireless Communications*, Volume 7, Issue 7, pp. 2640-2650, July 2008.

- [15] A. Khisti, A. Tchamkerten and G. W. Wornell, "Secure Broadcasting", available at http://arxiv.org/PS_cache/cs/pdf/0702/0702093v1.pdf.
- [16] E. Tekin, S. Serbetli, and A. Yener, "On secure Signaling for the Gaussian Multiple Access Wire-tap Channel", in *Proc. 2005 Asilomar Conf. On Signals, Systems, and Computers*, Asilomar, CA, pp. 1747-1751, November 2005.
- [17] E. Tekin and A. Yener, "The Gaussian Multiple Access Wire-Tap Channel", in *IEEE Trans. on Info. Theory*, Volume 54, Issue 12, pp. 5747-5755, Dec. 2008.
- [18] Y. Liang and V. Poor, "Generalized Multiple Access Channels with Confidential Messages", in *Proc. Of IEEE Int. Symp. Inf. Theory (ISIT)*, pp. 952-956, July 2006.
- [19] E. Tekin and A. Yener, "The Gaussian Multiple Access Wire-Tap Channel: Wireless Secrecy and Cooperative Jamming", *Information Theory and Applications Workshop*, pp. 404-413. Feb. 2007.
- [20] Y. Oohama, "Coding for Relay Channels with Confidential messages", in *Proc. Of IEEE Information Theory Workshop*, pp. 87-89, Sep. 2001.
- [21] Y. Oohama, "Capacity Theorems for Relay Channels with Confidential Messages", in *Proc. of ISIT 2007*, pp. 926-930, Jun. 2007.
- [22] L. Lai and H. El Gamal, "The Relay-Eavesdropper Channel: Cooperation for Secrecy", *IEEE Trans. Inf. Theory*, Volume 54, Issue 9, pp. 4005-4019, Sept. 2008.
- [23] M. Yuksel and E. Erkip., "The Relay Channel with a Wiretapper", in *Proc. Forty-First Annual Conference on Information Sciences and Systems (CISS)*, Baltimore, MD, USA, Mar. 2007.
- [24] Z. Li, R. Yates, and W. Trappe, "Secrecy Capacity of Independent Parallel Channels", in *Proc. 44th Annu. Allerton Conf. Communication, Control and Computing*, Monticello, IL, pp. 841-848, Sep. 2006.
- [25] F. Oggier, B. Hassibi, "The MIMO Wiretap Channel", *Communications, Control and Signal Processing, 2008. ISCCSP 2008. 3rd International Symposium on*, pp. 213-218, Mar. 2008.
- [26] S. Shafiee, L. Nan and S. Ulukus, "Secrecy Capacity of the 2-2-1 Gaussian MIMO Wire-tap Channel", *Communications, Control and Signal Processing, 2008. ISCCSP 2008. 3rd International Symposium on*, pp. 207-212, Mar. 2008.
- [27] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO Wiretap Channel", in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Nice, France, Jun. 2007.
- [28] A. Khisti and G. Wornell, "Secure Transmission with Multiple Antennas: The MISOME Wiretap Channel", available at http://arxiv.org/PS_cache/arxiv/pdf/0708/0708.4219v1.pdf.
- [29] T. Liu and S. Shamai (Shitz), "A Note on the Secrecy Capacity of the Multi-antenna Wiretap Channel", *IEEE Trans. Inf. Theory*, Volume 55, Issue 6, pp.2547 - 2553, June 2009.
- [30] R. Liu and H. V. Poor, "Multi-Antenna Gaussian Broadcast Channels with Confidential Messages", in *Proc. of ISIT 2008*, pp. 2202-2206, Jul. 2008.
- [31] R. Liu and H. V. Poor, "Secrecy Capacity Region of a Multi-Antenna Gaussian Broadcast Channels with Confidential Messages", *IEEE Trans. on Info. Theory*, Vol. 55, No. 3, pp. 1235-1249, Mar. 2009.
- [32] X. Tang, R. Liu, P. Spasojevic and V. Poor, "The Gaussian Wiretap Channel with a Helping Interferer", in *Proc. of ISIT 2008*, pp. 389-393, Jul. 2008.
- [33] C. Chan, "Success Exponent of Wiretapper: A Tradeoff between Secrecy and Reliability", available at http://arxiv.org/PS_cache/arxiv/pdf/0805/0805.3605v4.pdf.
- [34] X. Tang, R. Liu, P. Spasojevic and V. Poor, "Interference-Assisted Secret Communication", available at http://arxiv.org/PS_cache/arxiv/pdf/0804/0804.1382v1.pdf.
- [35] L. Lai, H. El-Gamal, V. Poor, "The Wiretap Channel With Feedback: Encryption Over the Channel", *IEEE Trans. Inf. Theory*, Volume 54, Issue 11, pp. 5059-5067, Nov. 2008.
- [36] O. Ozan Koyluoglu, H. El-Gamal, "On the Secure Degrees of Freedom in the K-User Gaussian Interference Channel", in *Proc. of ISIT 2008*, pp. 384-388, Jul. 2008.
- [37] S. I. Gelfand and M. S. Pinsker, "Coding for Channel with Random Parameters", *Problemy Peredachi Informatsii*, vol. 9, no. 1, pp. 19-31, 1980.
- [38] K. Marton, "A Coding Theorem for the Discrete Memoryless Broadcast Channel", *IEEE Trans. on Inf. Theory*, vol. 25, no. 1, pp. 306-311, May 1979.
- [39] T. Cover and J. Thomas, *Elements of Information Theory*. John Wiley Sons, Inc., 1991.
- [40] G. Bagherikaram, A. S. Motahari, A. K. Khandani "Secure broadcasting : The Secrecy Rate Region", in *Proc. of 46th Annual Allerton Conference on Communication, Control, and Computing*, pp. 834 - 841, 23-26 Sept. 2008
- [41] E. Ekrem, S. Ulukus "On Secure broadcasting", in *Proc. of 42nd Asilomar Conference on Signals, Systems and Computers*, pp. 676 - 680, 26-29 Oct. 2008.
- [42] E. Ekrem, S. Ulukus "Secrecy Capacity of a Class of Broadcast Channels with an Eavesdropper", available at http://arxiv.org/PS_cache/arxiv/pdf/0812/0812.0319v1.pdf.
- [43] E. Ekrem, S. Ulukus "Secrecy Capacity Region of the Gaussian Multi-Receiver Wiretap Channel", in *Proc. of IEEE International Symposium on Information Theory (ISIT)*, pp. 2612 - 2616, June 28 2009-July 3 2009
- [44] C. E. Shannon, "A mathematical Theory of Communication", *Bell Syst. Tech. J.*, vol. 27, pp. 379-423 and 623-656, Jul. and Oct. 1948
- [45] A. J. Stam, "Some Inequalities Satisfied by the Quantities of Information of Fisher and Shannon" *Information and Control*, vol. 2 pp. 101-112, Jun. 1959
- [46] S. N. Digavvi, T. M. Cover, "The Worst Additive Noise Under a Covariance Constraint", *IEEE Trans. on Info. Theory*, Vol. 47, No. 7, pp. 3072-3081, Nov. 2001.
- [47] T. Liu, P. Viswanath, "An Extremal Inequality Motivated by Multiterminal Information Theoretic Problems", *IEEE Trans. on Inf. Theory*, vol. 53, no. 5, pp. 1839-1851, May 2007.
- [48] M. H. M. Costa, "A New Entropy Power Inequality", *IEEE Trans. on Inf. Theory*, vol. 31, no. 6 pp. 751-760, Nov. 1985.
- [49] R. Liu, T. Liu, H. V. Poor, S. Shamai (Shitz), "A Vector Generalization of Costa Entropy Power Inequality and Applications", Submitted to *IEEE Trans. on Inf. Theory*, Mar. 2009.